Principles and Foundations for Fractionated Networked Cyber-Physical Systems

Quarterly Report

Carolyn Talcott Mark-Oliver Stehr Pat Lincoln

Date of Preparation: 7/13/2012
Period covered: Inception - 6/30/2012

Project Abstract A new generation of mission-critical systems is emerging that employs distributed, dynamically reconfigurable open architectures. These systems may include a variety of devices that sense and affect their environment and the configuration of the system itself. We call such systems *Networked Cyber-Physical Systems* (NCPS). NCPS can provide complex, situation-aware, and often critical services in applications such as distributed sensing and surveillance, crisis response, self-assembling structures or systems, networked satellite and unmanned vehicle missions, or distributed critical infrastructure monitoring and control. NCPS are of special interest to the Navy in view of the increasing need for coordination of a wide spectrum of maritime sensing and information gathering technologies, ranging from smart mobile buoys to autonomous underwater vehicles and their integration into a global network with maritime, space, and ground domains.

NCPS must be reactive and maintain an overall situation, location, and time awareness that emerges from the exchange of knowledge. They must achieve system goals through local, asynchronous actions, using (distributed) control loops through which the environment provides essential feedback. They must deal with uncertainty and partial knowledge, and be capable of a wide spectrum of operations between autonomy and cooperation to adapt to resource constraints and disruptions in communication. General principles and tools are needed for building robust, effective NCPS. A key observation is that the current level of abstraction at which software and systems are designed is a barrier to innovation at the hardware and networking level and at the same time is not suitable to enable rapid design/deployment or distributed control of large-scale distributed software systems and in particular the flexible, dynamically reconfigurable, mission-critical NCPS of the future.

We propose to explore a new paradigm for design of high-assurance NCPS based on the notion of software fractionation with declarative distributed control and optimization aiming at the effective use of resources. The idea of software fractionation is inspired by and complementary to hardware fractionation, which has been proposed for mission-critical space systems. Fractionation has the potential of leading to software that is more robust, leveraging both diversity and redundancy. It raises the level of abstraction at which control and optimization techniques are applied.

1 Technical Approach

In this project we adopt a view of cyber-physical systems that goes beyond the conventional definition of a hardware/software system that is interacting with the physical world. Our goal is to explore a new notion of software that behaves itself closer to a physical or biological system. In other words, we aim to address the fundamental problem by reducing the sharp boundary between physics and computation. Our rationale is that current models of distributed computing are too abstract by not taking into account fundamental physical limitations and hence are not efficiently implementable or scalable. Once limitations can be explicitly represented, they can be overcome to some degree, which can be quantified, e.g., probabilistically. Like in biological systems, diversification, redundancy, and randomization should be utilized to overcome physical limitations whenever possible. In particular, distribution is a source of redundancy and diversification that can be turned from an obstacle into an advantage.

In our approach, software is fractionated by design even beyond the distributed nature of underlying system, with distributed knowledge sharing as the underlying model. Computation and communication is not rigid but guided by the physical resources, e.g., in an opportunistic fashion. Our vision that fractionated software operates as an inherently open system in a highly redundant and diversified way avoiding single points of responsibilities and failure. Being resource-aware, fractionated software operates in the entire spectrum between autonomy to cooperation. Our distributed computing model is based on distributed knowledge sharing, and makes very few assumptions but restricts the shape of fractionated software so that it can run on a wide range of platforms. In particular it does not assume strong primitives that are powerful but not implementable in a scalable way.

2 Activities during this Quarter

Activities during this quarter comprise research on theoretical and practical foundations for fractionated cyber physical systems (FCPS) and work on our networked cyber-physical systems (NCPS) testbed, which both are a direct continuation of the work started in the previous quarter.

2.1 Research on Theoretical and Practical Foundations for FCPS

The vision of fractionated software is that distributed computations are mapped to resources at runtime in a flexible way without the need for a complex (global) coordination mechanism. If some components fail other components can step in and take over the computation without the need for explicit migration. Randomization techniques will make sure that enough diversity is maintained to allow reasonably efficient operation, e.g., to achieve performance and reliability constraints.

A key capability of Fractionated Cyber-Physical Systems (FCPS) is performance of goals with acceptable fault tolerance, energy consumption, confidence level and delay. To achieve this capability, each node in the FCPS must decide independently what actions to take. An important case is where the system goal can be reduced to a set of largely independent subgoals, and the actions of a node consist in selecting and executing subgoals. This decision process is a function of the parameters of the FCPS and its environment. We created an abstract model for this decision process, the Stochastic Task Execution Model (STEM), and examined its behavior to gain insight into an optimal task execution decision process for FCPS. Model parameters include the number of nodes, node connectivity and communications delay, the number of subgoals, desired goal coverage and confidence level. Monte Carlo simulation was carried out to investigate the effects of different parameter choices and requirements on efficiency (the number of subgoals covered divided by the number of subgoal executions), performance (efficiency divided by total effort = number of nodes times the time to completion). The ability of nodes to share knowledge is a key factor. In our simplified model, with sufficient communication a node to subgoal ratio between .5 and 1 provides close to optimal efficiency and performance.

2.2 Work on NCPS Testbed and Software Interfaces

We are continuing to develop a small UAV testbed consisting of 10 inexpensive quadcopters at SRI. Hardware-wise, we added heat sinks to mitigate the impact of additional heat that is caused by our modification with an additional on-board computer (Gumstix Overo Fire that comes with a WiFi module) as well as sensors such as a digital compass and a GPS module. Software-wise, the localization and navigation capabilities for a single UAV has been improved by coordinating the existing gyroscope and the attached GPS/compass and the accuracy has been tested in real world situations. We are currently in the process of integrating flight control software described in a format of workflow with our cyber-application framework for networked cyber-physical systems. As a first step, we tested position information exchange among UAVs that is based on the notion of partially ordered knowledge sharing model in the cyber-application framework. In the end, we expect that the additional on-board computer can be used to run high-level flight control software and the cyber-application framework with networking and workflow execution capabilities while an on-board embedded Linux system deals with low-level controls.

SRI INTERNATIONAL GRANT NO. N00014-10-1-0365

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
7/13/2012	Quarterly Report - Phase 2	Inception - 6/30/2012

4. TITLE AND SUBTITLE
Principles and Foundations for Fractionated Networked Cyber-Physical Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-10-1-0365

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dr. Mark-Oliver Stehr
Dr. Carolyn Talcott
Dr. Patrick Lincoln

5d. PROJECT NUMBER
11PR00456-05

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025-3493

8. PERFORMING ORGANIZATION REPORT NUMBER P20679 Qtr Incep-June 2012

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Naval Research
875 North Randolph Street
Arlington, VA 22203-1995

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release, Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
We are exploring a new paradigm for design of high-assurance Networked Cyber-Physical Systems based on the notion of software fractionation with distributed control and optimization aiming at the effective use of resources. The idea of software fractionation is inspired by and complementary to hardware fractionation, which has been proposed for mission-critical space systems. In our approach, software is fractionated by design even beyond the distributed nature of underlying system, with distributed knowledge sharing as the underlying model. In this report we summarize our research on a Stochastic Task Execution Model (STEM) designed to gain insight into design parameters of local decision processes to robustly meet system goals. We also report on our ongoing work on building an NCPS test bed at SRI based on quadricopter hardware.

15. SUBJECT TERMS
Fractionated Software, Distributed Computing, Networking, Cyber-Physical Systems

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
u	u	u	uu		Kathryn Tracy
					19b. TELEPHONE NUMBER *(include area code)* 650-859-3435

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18